# The Category CNOT

Robin Cockett [*] Cole Comfort Priyaa Srinivasan [†]
Department of Computer Science
and Institute for Quantum Science and Technology
University of Calgary
Alberta, Canada
robin@ucalgary.ca

We exhibit a complete set of identities for CNOT, the symmetric monoidal category generated by the controlled-not gate, the swap gate, and the computational ancillæ. We prove that CNOT is a discrete inverse category. Moreover, we prove that CNOT is equivalent to the category of partial isomorphisms of finitely-generated non-empty commutative torsors of characteristic 2. Equivalently this is the category of affine partial isomorphisms between finite-dimensional $\mathbb{Z}_2$ vector spaces.

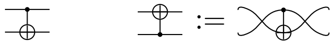
## 1 Introduction

In this paper, we model the behaviour of circuits comprised of cnot gates and the four computational ancillæ—which restrict certain inputs and outputs to be either 0 or 1. We model these circuits as maps in the symmetric monoidal category CNOT given by finite generators and relations. Although the cnot gate is unitary, the ancillæ are not. This is because ancillæ model state preparation and measurement which are irreversible operations. Ancilliæ are commonly used in quantum error correction codes [5, 9]; moreover, the proof that the Toffolli gate is universal uses ancillæ [14]. Although unitary transformations are an active area of research [10], and there is a finite, faithful set of identities for circuits composed of cnot gates [1], the structure of circuits composed of cnot gates *and* ancillæ is not yet studied.

This research extends the work of Lafont, who classified several similar categories [12]. We prove that CNOT is equivalent to a concrete category of torsors and partial maps – in other words the category of affine partial isomorphisms between finite dimensional $\mathbb{Z}_2$ vector spaces. We have yet to prove that there is a *faithful* embedding of CNOT into the category of dagger Frobenius Algebras in finite-dimensional Hilbert spaces and completely positive maps, CPM(FHilb) (see [13]).

## 2 Defining the Category CNOT

CNOT is a symmetric monoidal category presented by generating maps and identities. We use string diagrams to express the maps in CNOT. For the cnot-gate and the upside-down cnot-gate, we use the following notation respectively:



[*] partially supported by NSERC

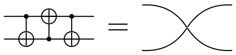
[†] partially supported by the NSERC grant of Dr. Barry C. Sanders

Bob Coecke and Aleks Kissinger (Eds.):
14th International Conference on Quantum Physics and Logic (QPL)
EPTCS 266, 2018, pp. 258–293, doi:10.4204/EPTCS.266.18

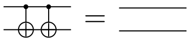
We call the wire of the cnot gate with the dot the **control bit** and the other wire with the $\oplus$ the **operating bit**. We graphically denote the input and output ancillary bits for 1 by ▸── and ──◂. Algebraically we denote the input ancillary bit for 1 by $|1\rangle$ and the output ancillary bit for 1 by $\langle 1|$.

CNOT is the symmetric monoidal category generated by cnot, and the 1 ancillæ satisfying the identities *(CNT.1)-(CNT.9)*. Two maps are the same in CNOT if and only if they can be transformed to another using the following identities:

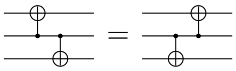
*(CNT.1)*



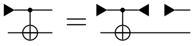
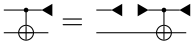
*(CNT.2)*



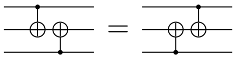
*(CNT.3)*



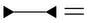
*(CNT.4)*

 and 

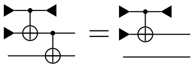
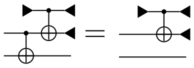
*(CNT.5)*



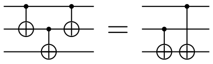
*(CNT.6)*



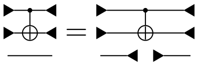
*(CNT.7)*

 and 

*(CNT.8)*



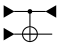
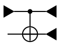
*(CNT.9)*



Note that all of the identities *(CNT.1)-(CNT.9)* are horizontally symmetric. This symmetry expresses a functorial involution which will be useful later.

While the first eight identities are quite familiar, *(CNT.9)* may be unexpected: it is reminiscent of the absorbing scalar Axiom *(ZO)* in the ZX calculus [3].

Note that CNOT only has 3 generating gates as we can construct the 0-ancillary bits from cnot and the 1 ancillary bits. The following gates are respectively the input and output 0 ancillary bits:

▹─ :=  and dually ─◃ := 

We denote these ancillary bits algebraically by $|0\rangle$ and $\langle 0|$ respectively.

## 2.1 Restriction and inverse categories

In this section, we introduce the basic theory and terminology of restriction categories which we use later.

**Definition 2.1.** *[6, Def. 2.1.1]*

*A* ***restriction structure*** *on a category $\mathbb{X}$ is an assignment $\overline{f} : A \to A$ for each map $f : A \to B$ in $\mathbb{X}$ satisfying the following four axioms:*

*(R.1)* $\overline{f} f = f$ *for every map $f$ in $\mathbb{X}$*

*(R.2)* $\overline{f}\,\overline{g} = \overline{g}\,\overline{f}$ *whenever* $\mathsf{dom} f = \mathsf{dom} g$ *for maps $f, g$ in $\mathbb{X}$.*

*(R.3)* $\overline{\overline{g} f} = \overline{f}\,\overline{g}$ *whenever* $\mathsf{dom} f = \mathsf{dom} g$ *for maps $f, g$ in $\mathbb{X}$.*

*(R.4)* $f\overline{g} = \overline{fg} f$ *whenever* $\mathsf{cod} f = \mathsf{dom} g$ *for maps $f, g$ in $\mathbb{X}$.*

A **restriction category** is a category equipped with a restriction structure. A **restriction functor** is a functor which preserves the restriction structure. An endomorphism $e : A \to A$ is called a **restriction idempotent** if $e = \overline{e}$. In particular, each $\overline{f}$ is an idempotent ($\overline{f}\,\overline{f} = \overline{\overline{f} f} = \overline{f}$) and $\overline{\overline{f}} = \overline{f}$.

In a restriction category, a **total map** is a map $f$ such that $\overline{f} = 1$. The total maps of a restriction category $\mathbb{X}$ form a subcategory $\mathsf{Total}(\mathbb{X})$ of $\mathbb{X}$.

A restriction category is a 2-category with 2-cells given by the partial order $f \leq g \iff f = \overline{f} g$. In particular, if $f$ and $g$ are restriction idempotents, then $f \leq g \iff f = fg$ [6, Sec. 2.1.4].

A basic example of a restriction categories is a partial map category. One can form a partial map category from any category which has pullbacks:

**Definition 2.2.** *[6, Sec. 3] Given a category $\mathbb{X}$ with pullbacks,* ***the category of partial maps*** *of $\mathbb{X}$, Par$(\mathbb{X})$ is defined as follows:*

**Objects:** *Objects in $\mathbb{X}$.*

**Maps:** *Every map from $A$ to $B$ is a pair $(m, f)$ such that $m : A' \to A$ and $f : A' \to B$ such that $m$ is monic—up to an equivalence relation $(m, f) \sim (m', f')$ if and only if there exists an isomorphism $\alpha$ such that $\alpha m' = m$ and $\alpha f' = f$.*

**Identities:** *The identity on $A$ is the pair $(1_A, 1_A)$.*

**Composition:** *For maps $(m, f) : A \to B$ and $(m', g) : B \to C$, $(m, f)(m', g) := (m'' m, f' g)$ where $m''$ and $f'$ are determined by the following pullback:*

$$\begin{tikzcd}
 & & A'' \arrow[dl, "m''"'] \arrow[dr, "f'"] \arrow[dd, phantom, very near start, "\vee"] & & \\
 & A' \arrow[dl, "m"'] \arrow[dr, "f"] & & B' \arrow[dl, "m'"'] \arrow[dr, "g"] & \\
A & & B & & C
\end{tikzcd}$$

*Composition is well-defined even though pullbacks are determined only up to isomorphism as the maps are taken modulo the equivalence relation.*

$\mathsf{Par}(\mathbb{X})$ *is endowed with a restriction structure by $\overline{(m, f)} := (m, m)$.*

The notion of a partial map category can be generalized by restricting the monics to any class of monics closed to composition, isomorphisms and pullbacks [6, Sec. 3]. However, here we consider only the class of all monics.

**Definition 2.3.** *[6, Sec. 2.3] A map $f$ is a **partial isomorphism** when there exists another map $g$, called the **partial inverse** of $f$, such that $\overline{f} = fg$ and $\overline{g} = gf$.*

Partial isomorphisms generalize the notion of an isomorphisms to restriction categories; thus, the composition of partial isomorphisms is a partial isomorphism and partial inverses are unique. A restriction category $\mathbb{X}$ is an **inverse category** when all its maps are partial isomorphisms. A one object inverse category is an inverse monoid.

Given any restriction category $\mathbb{X}$, there is a subcategory of partial isomorphisms of $\mathbb{X}$, denoted by $\mathsf{ParIso}(\mathbb{X})$ which is an inverse category.

There is an important alternate way to view an inverse category:

**Theorem 2.4.** *[6, Thm. 2.20] A category $\mathbb{X}$ is an inverse category if and only if there exists an involution $(\_)^\circ : \mathbb{X}^{op} \to \mathbb{X}$ which is the identity on objects, satisfying the following three axioms:*

*(Inv.1)* $(c^\circ)^\circ = c$

*(Inv.2)* $cc^\circ c = c$

*(Inv.3)* $cc^\circ dd^\circ = dd^\circ cc^\circ$

Inverse categories have restriction structure given by $\overline{c} := cc^\circ$. It is not hard to show that every idempotent in an inverse category is necessarily a restriction idempotent.

## 2.2 Discrete restriction categories and inverse products

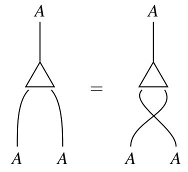
If a category $\mathbb{X}$ has products then $\mathsf{Par}(\mathbb{X})$ has restriction products: these are "lax" products for which the pairing operation satisfies $\langle f,g\rangle\pi_0 = \overline{g}f$ (and $\langle f,g\rangle\pi_1 = \overline{f}g$). If the category $\mathbb{X}$ has a final object then $\mathsf{Par}(\mathbb{X})$ has a restriction final object, that is an object ! for which, for each object $A$, there is a unique total map $! : A \to 1$ so that for any map $k : A \to 1$, $k = \overline{k}\,!$. A restriction category with restriction products and a restriction terminal object is called a **Cartesian restriction category**.

A Cartesian restriction category in which the diagonal map, $\Delta_A : A \to A \times A$, is a partial isomorphism is called a **discrete Cartesian restriction category**. The partial map category, $\mathsf{Par}(\mathbb{X})$, of a category with products and pullbacks is always a discrete Cartesian restriction category (as the diagonal map is a partial isomorphism). Discrete Cartesian restriction categories are equivalently characterized as those Cartesian restriction categories which have meets:

**Definition 2.5.** *[8, Def. 4.3.1] Given an inverse category $\mathbb{X}$ equipped with a tensor product $\_\otimes\_ : \mathbb{X}\times\mathbb{X} \to \mathbb{X}$ which preserves $(\_)^\circ$, we say $\mathbb{X}$ has **inverse products** if there exists a total natural diagonal transformation $\Delta$ which satisfies the properties:*

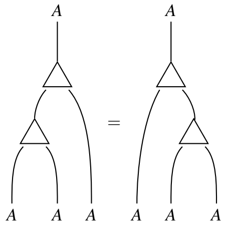
*(DInv.1) $\Delta$ is cocommutative for each $A \in \mathbb{X}$:*

$$\begin{tikzcd}
A \arrow[r, "\Delta_A"] \arrow[dr, "\Delta_A"'] & A\otimes A \arrow[d, "c_{A,A}"] \\
& D
\end{tikzcd}$$



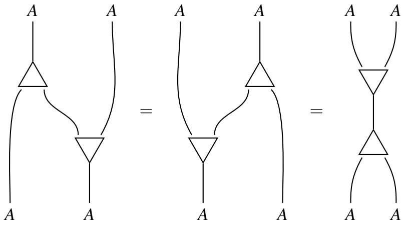
*(DInv.2)* $\Delta$ *is coassociative for each* $A \in \mathbb{X}$*:*

$$\begin{tikzcd}
A \arrow[rr, "\Delta_A"] \arrow[d, "\Delta_A"'] & & A \otimes A \arrow[d, "1_A \otimes \Delta_A"] \\
A \otimes A \arrow[dr, "\Delta_A \otimes 1_A"'] & & A \otimes (A \otimes A) \\
& (A \otimes A) \otimes A \arrow[ur, "a_{A,A,A}"'] &
\end{tikzcd}$$



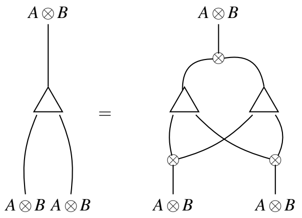
*(DInv.3)* $(\Delta, \Delta^\circ)$ *is a semi-Frobenius object for each* $A \in \mathbb{X}$*:*

$$\begin{tikzcd}
A \otimes A \arrow[rr, "(\Delta_A \otimes 1_A)a_{A,A,A}"] \arrow[dr, "\Delta_A^\circ"] \arrow[dd, "(1_A \otimes \Delta_A)a^\circ_{A,A,A}"'] & & A \otimes (A \otimes A) \arrow[dd, "1_A \otimes \Delta_A^\circ"] \\
& A \arrow[dr, "\Delta_A"] & \\
(A \otimes A) \otimes A \arrow[rr, "\Delta_A^\circ \otimes 1_A"] & & A \otimes A
\end{tikzcd}$$



*(DInv.4)* $\Delta$ *satisfies the uniform copying identity for each* $A, B \in \mathbb{X}$*:*

$$\begin{tikzcd}
A \otimes B \arrow[rr, "\Delta_A \otimes \Delta_B"] \arrow[dr, "\Delta_{A \otimes B}"'] & & (A \otimes A) \otimes (B \otimes B) \arrow[dl, "\mathsf{ex}_{A,B}"] \\
& (A \otimes B) \otimes (A \otimes B) &
\end{tikzcd}$$



Where the natural isomorphism,

$$\mathsf{ex} := a(1 \otimes a^\circ)(1 \otimes (c \otimes 1))((1 \otimes a)a^\circ) : (A \otimes B) \otimes (C \otimes D) \to (A \otimes C) \otimes (B \otimes D)$$

is called the exchange map.

A **discrete inverse category** is an inverse category with inverse products. Note that $\Delta$ is total if and only if $\Delta$ is separable (special), that is, $\Delta\Delta^\circ = 1$. A discrete inverse category always has meets [8]: $f \cap g := \Delta(f \otimes g)\Delta^\circ$. Furthermore, the partial isomorphisms of a discrete Cartesian restriction category (such as $\mathsf{Par}(\mathbb{X})$ for a $\mathbb{X}$ with finite limits) is always a discrete inverse category. Conversely – and more surprisingly – every discrete inverse category has a "completion" to a discrete Cartesian restriction category (see [8] for more details).

## 3 Torsors

We will prove that CNOT is equivalent to the category of partial isomorphism between finitely generated non-empty commutative torsors of characteristic 2, $\mathsf{ParIso}(\mathsf{CTor}_2)^*$. Torsors are essentially groups without a fixed multiplicative identity: the category $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ may, thus, also be viewed as the partial isomorphism category of finite-dimensional $\mathbb{Z}_2$ vector spaces with affine maps.

**Definition 3.1.** *A **torsor** is a set $X$ along with a ternary operator $(\_)\times_{(\_)}(\_) : X \times X \times X \to X$ called para-multiplication, such that for any $a,b,c,d,e \in X$, the following laws hold [11]:*

**Para-associative law:**

$$(a \times_b c) \times_d e = a \times_{d \times_c b} e = a \times_b (c \times_d e)$$

**Para-identity law:**

$$a \times_b b = b \times_b a = a$$

A torsor is said to be **commutative**, when $a \times_b c = c \times_b a$. A torsor is said to have **characteristic 2**, when $a \times_b a = b$.

The category of torsors $\mathsf{Tor}$ has objects torsors and maps homomorphisms of torsors. A homomorphisms of torsors, $f : (X,\times) \to (Y,\times)$, is a functions $X \to Y$ which preserve para-multiplication. As this is a category of algebras we know that it is a finitely complete category. This allows us to form $\mathsf{Par}(\mathsf{Tor})$ and $\mathsf{ParIso}(\mathsf{Tor})$ immediately.

Note that the empty set is a torsor, however, if $(X,\times)$ is a non-empty torsor, then $X$ has, for each element of $X$, a group structure. Thus, given any $z \in X$, $X$ is a group under the multiplication

$$\_\cdot\_ : X^2 \to X; (x,y) \mapsto x \times_z y.$$

Conversely, if $(X,\cdot)$ is a group, then $X$ has a non-empty torsor structure $\_\times_{\_}\_ : X^3 \to X$ such that $(x,z,y) \mapsto x \cdot z^{-1} \cdot y$ [4, Sec. 0.2]. Note that this correspondence does not imply that the category of torsors and groups are equivalent since their homomorphisms are different.

Some authors, including their originator [11, Def. 18], require the underlying set of a torsor to be nonempty so that torsors always arise as groups. However, following [4, Sec. 0.2], we will not impose this condition as we need a category closed to pullbacks, and the empty torsor arises as a pullback. A torsors is also also known as a "... heap, groud, flock, herd, principal homogeneous space, abstract coset, pregroup ..." [4, Sec. 0.2] with the non-emptiness condition appearing in some cases.

**Definition 3.2.** *Define $\mathsf{CTor}_2$ to be the full subcategory of torsors whose objects are finitely generated commutative torsors of characteristic 2 (including the empty torsor).*

There is an equivalent characterization of the objects of $\mathsf{CTor}_2$.

**Proposition 3.3.** *Every object in $\mathsf{CTor}_2$ is either empty or isomorphic to a finite dimensional $\mathbb{Z}_2$ vector spaces; furthermore, torsor homomorphisms are precisely the affine maps.*

*Proof.* Suppose that $X$ is a finitely generated commutative torsor under the para-multiplication $\_\times_{\_}\_ :$ $X^3 \to X$. If $X$ is nonempty, fix some element $z \in X$. As $X$ has characteristic 2 as a commutative torsor, it has characteristic 2 as a Abelian group under the addition $\_+\_ := \_\times_z\_ : X^2 \to X$. Furthermore, the dimension of such a torsor is one more than the dimension of this corresponding group (as the base point must be added). Thus, finitely generated commutative torsors of characteristic 2 are finite. Therefore, by the fundamental theorem of finitely generated Abelian groups:

$$X \cong \mathbb{Z}^0 \oplus \left( \bigoplus_{i=1}^{n} \mathbb{Z}_2 \right) \cong \mathbb{Z}_2^n$$

with para-multiplication given by:

$$(a,b,c) \mapsto a \oplus (-b) \oplus c = a \oplus b \oplus c$$

Given a morphism of non-empty torsors, $f : (\mathbb{Z}_2^n, \_ \oplus \_ \oplus \_) \to (\mathbb{Z}_2^m, \_ \oplus \_ \oplus \_)$, for any $x$ and $y$ in $\mathbb{Z}_2^n$,

$$f(x \oplus y) = f(x \oplus 0 \oplus y) = f(x) \oplus f(y) \oplus f(0)$$

Therefore, $f$ is an affine transformation when $\mathbb{Z}_2^n$ and $\mathbb{Z}_2^m$ are seen as vector spaces over $\mathbb{Z}_2$.

Conversely, consider an affine transformation of vector spaces $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. Then $f$ can be regarded as morphism of torsors as for any $x, y, z \in \mathbb{Z}_2^n$,

$$\begin{aligned} f(x \oplus y \oplus z) &= f(x \oplus (y \oplus z)) = f(x) \oplus f(y \oplus z) \oplus f(0) \\ &= f(x) \oplus f(y) \oplus f(z) \oplus f(0) \oplus f(0) \\ &= f(x) \oplus f(y) \oplus f(z) \end{aligned}$$

The empty torsor and the empty affine space are strict initial objects; therefore, they have the same maps in torsors and Abelian groups viewed as affine spaces. □

As $\mathsf{CTor}_2$ is a category of algebras and so is finitely complete, we may construct $\mathsf{Par}(\mathsf{CTor}_2)$ and $\mathsf{ParIso}(\mathsf{CTor}_2)$. Let $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ denote $\mathsf{ParIso}(\mathsf{CTor}_2)$ without the empty torsor.

**Proposition 3.4.** $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ *is a discrete inverse category.*

*Proof.* $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ is an inverse category by construction. Because $\mathsf{Par}(\mathsf{CTor}_2)^*$ is a discrete Cartesian restriction category and $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ is the category of partial isomorphisms, it therefore has inverse products (see [8, Theorem 4.3.7]). Thus, it is a discrete inverse category. □

One further property of $\mathsf{CTor}_2$ is worth mentioning: all its monic maps are *regular* monics. This means, more concretely, every subobject of a torsor is determined by some set of equations. This then means that in $\mathsf{Par}(\mathsf{CTor}_2)^*$ the restriction idempotents correspond to equations.

## 4 Overview of Proof

The main theorem of this paper is:

**Theorem** C.27
*There is an equivalence of categories between* CNOT *and* $\mathsf{ParIso}(\mathsf{CTor})^*$.

The equivalence is shown in the following steps:

1. Proof that CNOT is a discrete inverse category.

   The first major challenge is to prove that CNOT is a discrete inverse category. We approach this by setting up the “discrete” part of the structure first. For this, we construct the “copy” natural transformation $\Delta$ which is defined inductively. The base case of 1 wire is defined by applying a cnot gate to a 0 ancillary bit. Then we prove that $\Delta$ has the properties required by an inverse product. This involves showing that the family of maps $\{\Delta_n : n \to 2n\}_{n\in\mathbb{N}}$ is a natural transformation i.e., for any circuit $f : n \to m$ in CNOT, $f\Delta_m = \Delta_{2n}(f \otimes f)$. Naturality of $\Delta$ is proven by a structural induction on $f$. Next, we prove that $\Delta$ forms a total semi-Frobenius algebra.

   CNOT has an important symmetry expressed by a functor $(\_)^\circ : \mathsf{CNOT}^{\mathrm{op}} \to \mathsf{CNOT}$ which “horizontally flips” maps (circuits). We use this functor to prove that CNOT is an inverse category.

2. Construction of a functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$.

   Our final objective is to prove that the category of partial isomorphisms between non-empty, finitely generated commutative torsors of characteristic 2, $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ is equivalent to $\mathsf{CNOT}$. In order to establish this, we construct a functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ indirectly by constructing a functor $h_0 : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{Set})$. We show that $h_0$ can be factored in two ways:

   - Through the inclusion $\iota : \mathsf{ParIso}(\mathsf{Set}) \to \mathsf{Par}(\mathsf{Set})$
   - Through the underlying functor $\mathsf{Par}(U) : \mathsf{Par}(\mathsf{CTor}_2)^* \to \mathsf{Par}(\mathsf{Set})$

   These factorizations imply $H_0$ factors through the pullback of $\iota$ and $\mathsf{Par}(U)$ which is $\mathsf{ParIso}(\mathsf{CTor}_2)^*$. Thus, we obtain a map $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$.

   There is another important way to describe this functor: as $\mathsf{CNOT}$ is the freely generated symmetric monoidal category on the gates cnot, $|1\rangle$, and $\langle 1|$, it suffices to interpret these into the category $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ and check that all of the identities hold. The result is equivalent to the functor we have produced and has the virtue of showing fairly immediately that $\tilde{H}_0$ preserves discrete inverse structure.

   Once we have proven that the functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ is well-defined, we prove that it an equivalence of categories. That is, that it is full, faithful, and essentially surjective. The proofs are in Appendix C. The essential surjectivity is straightforward; however, the other two are not.

3. Proof that $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ is a full functor.

   To obtain the fullness we need to show that any partial isomorphism between torsors can be simulated using circuits in $\mathsf{CNOT}$. However, we first show that we can simulate the graph, $\langle 1, f\rangle$, of a total map $f$ between torsors (see Lemma C.22). Next we observe that any partial map between torsors is dominated by a total map: so we can simulate the graph of this total map. The difficulty is now to introduce the partiality. To achieve this we use the fact that the functor is full on restriction idempotents (see Theorem C.19 - more on this soon): this allows us to simulate $\langle \overline{f}, f\rangle$ for any partial map $f$. However, by a general result (see Lemma C.21) we observe that simulating graphs of partial isomorphisms is sufficient to ensure we can simulate any partial isomorphism.

4. Proof that $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ is a faithful functor.

   To secure faithfulness we start by reducing the problem to showing faithfulness on restriction idempotents. This involves two observations. First we prove that a functor from an inverse category is faithful if and only if it is faithful on restriction idempotents and reflects them (see Lemma C.24). Next, we prove that a functor between discrete inverse categories which preserves the inverse product structure and is faithful on restriction idempotents always reflects restriction idempotents and, thus, is faithful (see Lemma C.25). Thus to establish faithfulness in our case it suffices to prove that $\tilde{H}_0$ is faithful on restriction idempotents.

   Toward this end we introduce a normal form, called "clausal form", for restriction idempotents in $\mathsf{CNOT}$ (Definition C.15). A circuit is in clausal form if and only if it is the composite of a finite number of clauses. A clause is a wire starting and ending with ancillary bits which is controlled from the identity (on $n$ wires). It has the effect of restricting the "legal" throughputs on the identity. Clauses correspond to torsor equations and can be manipulated by Gaussian elimination: and this means they are in bijective correspondence to the restriction idempotents in $\mathsf{ParIso}(\mathsf{CTor}_2)^*$. This is the content of Theorem C.19 which is the crux of the proof of Theorem C.27.

# 5 Concluding Remarks

In this work, we provided a complete set of identities for CNOT, the symmetric monoidal category generated by the cnot gate and the computational ancillæ. We proved that CNOT is equivalent to the category of partial isomorphisms of non-empty finitely generated commutative torsors of characteristic 2, $\mathsf{ParIso}(\mathsf{CTor}_2)^*$.

To the best of our knowledge, our work is the first to provide a complete set of identities for the cnot gate and computational ancillæ. The proof we present shows that CNOT is equivalent to a certain category of torsors. This we admit leaves a gap as one might expect a faithful functor from CNOT to CPM(FHilb), the category of finite dimensional Hilbert spaces with completely positive maps. Furthermore, as this embedding factors through the subcategory of stabilizer circuits which is equivalent to the ZX-calculus [2], there should also be a *faithful* embedding of CNOT into the ZX-calculus.

**Acknowledgements:**

We are very grateful to the referees who not only provided many useful comments but also were able to see in our first – and very rough – version of this paper that a complete proof might be hiding within!

# References

[1] Matthew Amy, Jianxin Chen & Neil J. Ross (2017): *A finite presentation of CNOT-dihedral operators*. ArXiv e-prints. `https://arxiv.org/abs/1701.00140`.

[2] Miriam Backens (2014): *The ZX-calculus is complete for stabilizer quantum mechanics*. New Journal of Physics 16(9), p. 093021, doi:10.1088/1367-2630/16/9/093021.

[3] Miriam Backens, Simon Perdrix & Quanlong Wang (2016): *A simplified Stabilizer zx-calculus*. arXiv preprint *arXiv:1602.04744*, doi:10.4204/EPTCS.236.1.

[4] Wolfgang Bertram & Michael Kinyon (2009): *Associative geometries. I: Torsors, linear relations and grassmannians*. arXiv preprint arXiv:0903.5441. `https://arxiv.org/abs/0903.5441`.

[5] John Chiaverini, Dietrich Leibfried, Tobias Schaetz, Murray D. Barrett, Bradford R. Blakestad, Joseph W. Britton, Wayne M. Itano, John D. Jost, Emanuel Knill, Christopher Langer et al. (2004): *Realization of quantum error correction*. Nature 432(7017), pp. 602–605, doi:10.1103/PhysRevLett.81.1525.

[6] J. Robin B. Cockett & Stephen Lack (2002): *Restriction categories I: categories of partial maps*. Theoretical computer science 270(1), pp. 223–259, doi:10.1016/S0304-3975(00)00382-0.

[7] Bob Coecke & Ross Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics*. New Journal of Physics 13(4), p. 043016, doi:10.1088/1367-2630/13/4/043016.

[8] Brett Giles (2014): *An investigation of some theoretical aspects of reversible computing*. Ph.D. thesis. `http://pages.cpsc.ucalgary.ca/~robin/Theses/BrettGilesPhD.pdf`.

[9] Daniel Gottesman (1997): *Stabilizer codes and quantum error correction*. arXiv preprint quant-ph/9705052. `https://arxiv.org/abs/quant-ph/9705052`.

[10] Martin Idel & Michael M. Wolf (2014): *Sinkhorn normal form for unitary matrices*. doi:10.1016/j.laa.2014.12.031.

[11] Maxim Kontsevich (1999): *Operads and motives in deformation quantization*. Letters in Mathematical Physics 48(1), pp. 35–72, doi:10.1023/A:1007555725247.

[12] Yves Lafont (2003): *Towards an algebraic theory of Boolean circuits*. Journal of Pure and Applied Algebra 184, p. 2003, doi:10.1016/S0022-4049(03)00069-0.

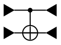
[13] Peter Selinger (2007): *Dagger compact closed categories and completely positive maps*. Electronic Notes in Theoretical Computer Science 170, pp. 139–163, doi:10.1016/j.entcs.2006.12.018.

[14] Siyao Xu (2015): *Reversible Logic Synthesis with Minimal Usage of Ancilla Bits*. *ArXiv e-prints.* `https://arxiv.org/abs/1506.03777`.

# A Preliminary results for CNOT

Because of Axiom *(CNT.9)*, certain circuits can interfere with the circuits with which they are tensored. This peculiar behaviour warrants discussion as these circuits are important later.

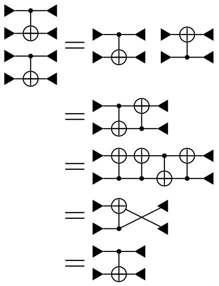
**Definition A.1.** *The* ***degenerate circuit*** *in* CNOT *is:*

$\Omega :=$  $: 0 \to 0$

This circuit consumes itself in the following sense:

**Lemma A.2.** $\Omega \otimes \Omega = \Omega$

*Proof.* We observe:



*(CNT.4)* × 2

*(CNT.2)*

*(CNT.1)*

□

We may generalize $\Omega$ to an arbitrary domain and codomain:

**Definition A.3.** *For any $n$ and $m$ in $\mathbb{N}$, define the degenerate circuit from $n$ to $m$, $\Omega_{n,m} : n \to m$ by the circuit* $(\otimes^n \langle 1|)\Omega(\otimes^m |1\rangle)$.

*Note that $\otimes^n\_$ denotes the $n$-fold iterated tensor product.*

These circuits exhibit the following "absorbing" property similar to Axiom *(ZO)* in the ZX calculus [3, 7]:

**Lemma A.4.**

*(i) If $f = f \otimes \Omega$, for some $f : n \to m$ then $f = \Omega_{n,m}$*

*(ii) If $g : m \to p$, then $\Omega_{n,m} g = \Omega_{n,p}$*

*(iii) If $h : p \to n$, then $h\Omega_{n,m} = \Omega_{p,n}$*

*Proof.*

(i) Consider an arbitrary circuit $f : n \to m$ such that $f = f \otimes \Omega$. Use *(CNT.9)* to cut the wires around every gate in $f$. Then every cut gate must either be $\Omega$ or $|1\rangle\langle 1|$. In the first case, use Lemma A.2 to consume the $\Omega$ obtained by cutting. In the second case, by *(CNT.6)*, allow one to remove the circuit. Thus $f = f \otimes \Omega = \Omega_{n,m}$.

(ii) Clearly $\Omega_{n,m}\Omega = \Omega_{n,m} \otimes \Omega = \Omega_{n,m}$ but then $h\Omega_{n,m} = (h\Omega_{n,m})\Omega$ so $h\Omega_{n,m} = \Omega_{p,m}$.

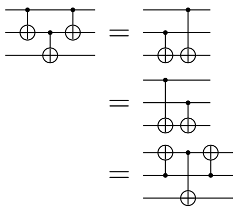
(iii) Dual to (ii).

□

Next, we prove some identities that will be used later to simplify proofs:

**Lemma A.5.**

*(i)*

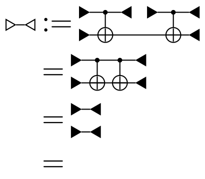


*(CNT.8)*

*(CNT.5)*

*(CNT.8)*

*(ii)*

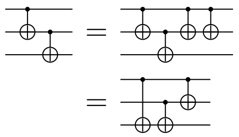


*(CNT.4)*

*(CNT.2)*

*(CNT.6)*

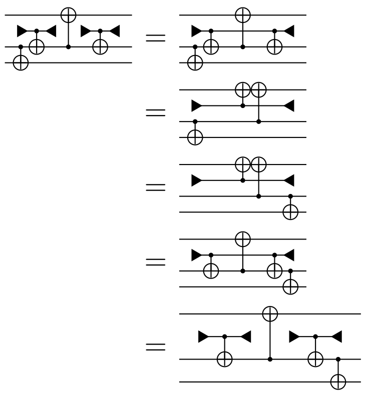
*(iii)*



*(CNT.2)*

*(CNT.8)*

*(iv)*



*(CNT.4)*

*(CNT.8)*

*(CNT.3)*

*(CNT.8)*

*(CNT.4)*

# B CNOT is a Discrete Inverse Category

In this section, we prove that CNOT is a discrete inverse category. We show discreteness before establishing the inverse category properties.

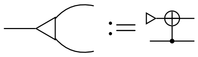
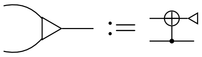
## B.1 Inverse products in CNOT

We begin by defining two families of maps $\Delta_n$ and $\nabla_n$ for all $n \in \mathbb{N}$. Then we show that $\Delta$ is coassociative and satisfies uniform copying law. $\Delta$ and show that $\Delta$ is a copy natural transformation which forms a cosemigroup such that the uniform copying law holds.

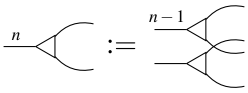
**Definition B.1.** *Define two families of maps* $\{\Delta_n : n \to 2n\}_{n\in\mathbb{N}}$ *and* $\{\nabla_n : 2n \to n\}_{n\in\mathbb{N}}$ *as follows.*

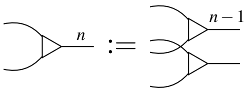
*On zero wires, define* $\Delta_0 := 1_0$.

*On one wire, define* $\Delta_1$, $\nabla_1$, *respectively by:*

 *and dually* 

*On n wires define* $\Delta$, $\nabla$ *inductively as follows:*



*and dually* 

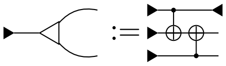
As we have defined CNOT by its generators, most of the proofs which follow involve structural induction.

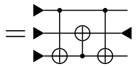
**Definition B.2.** *For any circuit f we define the size of the circuit* $|f|$ *as the number of* cnot *gates and ancillæ in* $f$.

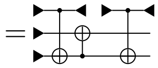
**Lemma B.3.** $\Delta$ *is a natural transformation.*

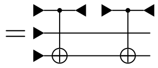
*Proof.* We prove $\Delta$ is natural by a structural induction on circuits.

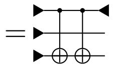
- For $|1\rangle$:

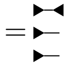


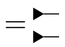
 *(CNT.8)*

 *(CNT.4)*

 *(CNT.7)*

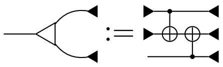
 *(CNT.4)*

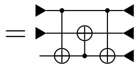
 *(CNT.2)*

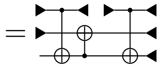
 *(CNT.6)*

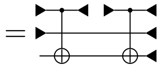
Therefore, $|1\rangle = \Delta_1(|1\rangle \otimes |1\rangle)$.

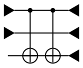
- For $\langle 1|$:

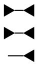


 *(CNT.8)*

 *(CNT.4)*

 *(CNT.7)*

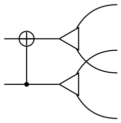
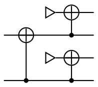
=  *(CNT.4)*

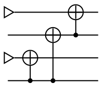
=  *(CNT.2)*

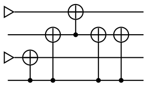
= *(CNT.6)* × 2

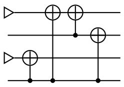
Therefore, $\langle 1| = \Delta_1(\langle 1| \otimes \langle 1|)$.

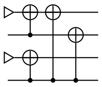
- For $\mathsf{cnot}$:

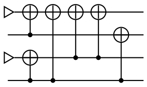
 := 

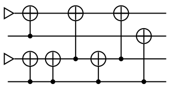
=  *(CNT.3)*

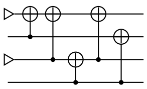
=  *(CNT.2)*

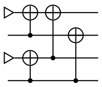
=  *(CNT.8)*

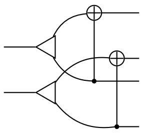
=  *(CNT.5)*

=  *(CNT.2)*

=  *(CNT.8)*

=  *(CNT.2)*

=  *(CNT.8)*

=: 

Therefore, $\mathsf{cnot} = \Delta_2(\mathsf{cnot} \otimes \mathsf{cnot})$.

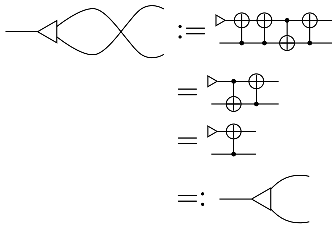
Therefore, $\Delta$ is natural by structural induction. □

**Lemma B.4.** $\Delta$ *is cocommutative.*

*Proof.* We prove that $\Delta$ is cocommutative by induction on the number of wires:

- On no wires the result is immediate.

- On one wire:

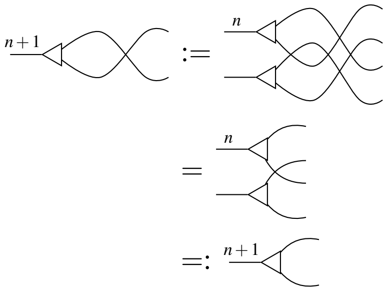


*(CNT.1)*

*(CNT.2)*

*(CNT.7)*

- Suppose inductively that $\Delta$ is cocommutative on up to $n$ wires. On $n+1$ wires:



By the inductive hypothesis

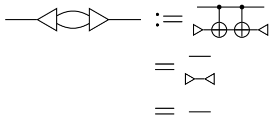
Therefore, the inductive claim holds.

□

**Lemma B.5.** $\Delta$ *is separable (or special).*

*Proof.* We prove that $\Delta$ is separable by induction on the number of wires.

- On zero wires it is the identity.
- On one wire:

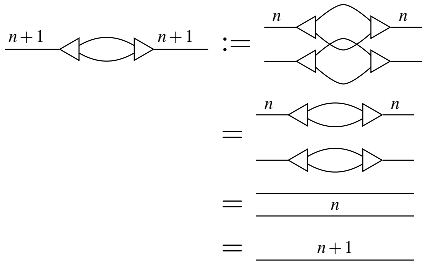


*(CNT.2)*

Lemma A.5 (ii)

Therefore, the base case on one wire holds.

- Suppose inductively that $\Delta_n \nabla_n = 1_n$ for some $n \in \mathbb{N}$. On $n+1$ wires:



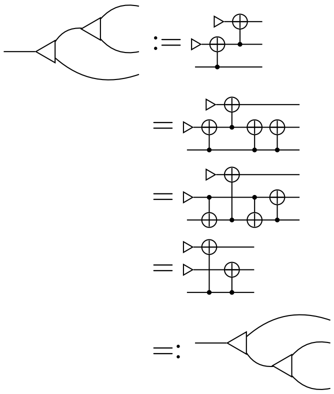
By the inductive hypothesis

□

**Lemma B.6.** $\Delta$ *is coassociative.*

*Proof.* We prove that $\Delta$ is coassociative by induction on the number of wires.

- On zero wires it is immediate.
- On one wire:



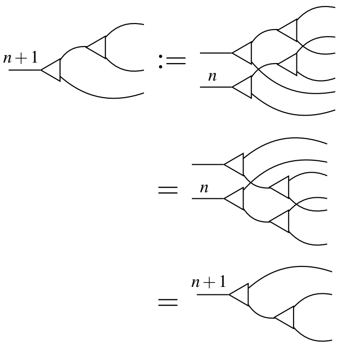
*(CNT.2)*

Lemma A.5 (i)

*(CNT.7)* × 2

Therefore, the base case on one wire holds.

- Suppose that $\Delta$ is coassociative on up to $n$ wires. On $n+1$ wires:



By the inductive hypothesis

Therefore, the inductive claim holds.

□

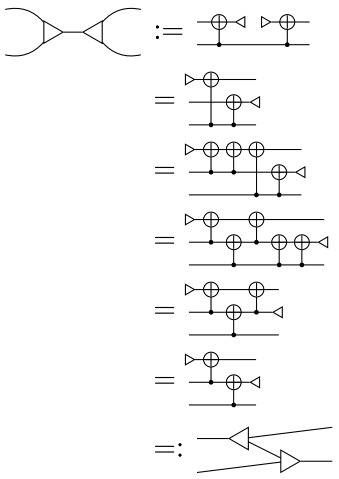
The dual propositions for $\nabla$ hold since, $\Delta^\circ = \nabla$.

**Lemma B.7.** $(n, \Delta_n, \nabla_n)$ *is a semi-Frobenius algebra for all* $n \in \mathbb{N}$.

*Proof.* We prove that $(\Delta, \nabla)$ is a semi-Frobenius algebra by induction on the number of wires.

- On one wire it is immediate.

- On one wire:



*(CNT.3)*

*(CNT.2)*

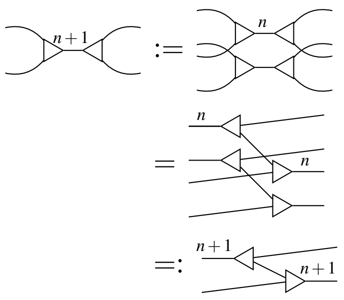
*(CNT.8)*

*(CNT.2)*

*(CNT.8)*

Therefore, the base case on one wire holds.

- Suppose inductively that $\Delta$ is semi-Frobenius algebra on up to $n$ wires. On $n+1$ wires:



By the inductive hypothesis

Therefore, the inductive claim holds.

□

**Lemma B.8.** *(DInv.4) holds for $\Delta$.*

*Proof.* The uniform copying law holds for $\Delta$ by construction. □

## B.2 CNOT is an inverse category

To prove that CNOT is an inverse category, we need to prove that the functor $(\_)^\circ : \mathsf{CNOT}^{\mathrm{op}} \to \mathsf{CNOT}$ which horizontally flips circuits satisfies *(Inv.1)*, *(Inv.2)* and *(Inv.3)*. It is immediate that *(Inv.1)* holds. It remains to show that *(Inv.2)* and *(Inv.3)* hold.

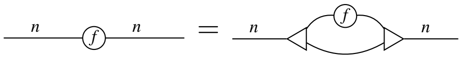
### B.2.1 Latchable Circuits

In order to prove that *(Inv.2)* holds, we identify the restriction idempotents $ff^\circ$ in CNOT with what we call "latchable circuits". We then show that for every $f$ that map $ff^\circ$ is latchable.

**Definition B.9.** *A circuit $f : n \to n$ is **latchable** when*

$$f = \Delta_n(f \otimes 1_n)\nabla_n$$

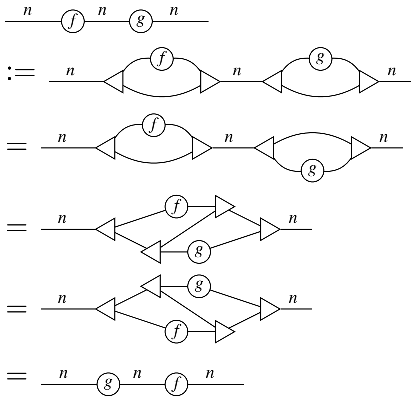
*That is, when the following holds:*



In order to use Theorem 2.4 to prove that CNOT is a discrete inverse category, we require the following:

**Lemma B.10.** *Latchable circuits commute and are idempotent.*

*Proof.* Suppose two circuits $f, g : n \to n$ are latchable, then:



By supposition

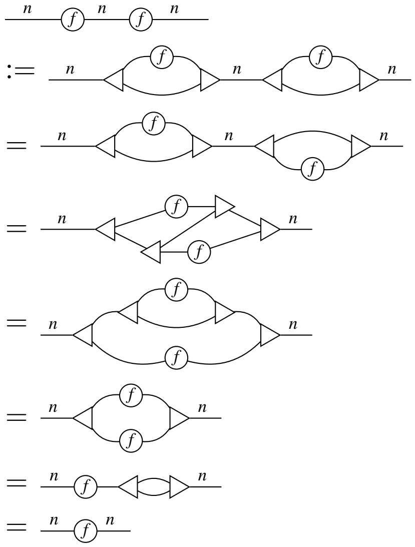
As $\Delta$ is commutative and cocommutative

As $\Delta$ is a semi-Frobenius algebra

As $\Delta$ is associative and coassociative

By symmetry

Therefore, latchable circuits commute. Likewise, by a similar argument:



By supposition

As $\Delta$ is commutative and cocommutative

As $\Delta$ is a semi-Frobenius algebra

As $\Delta$ is associative and coassociative

By supposition

As $\Delta$ is a natural transformation

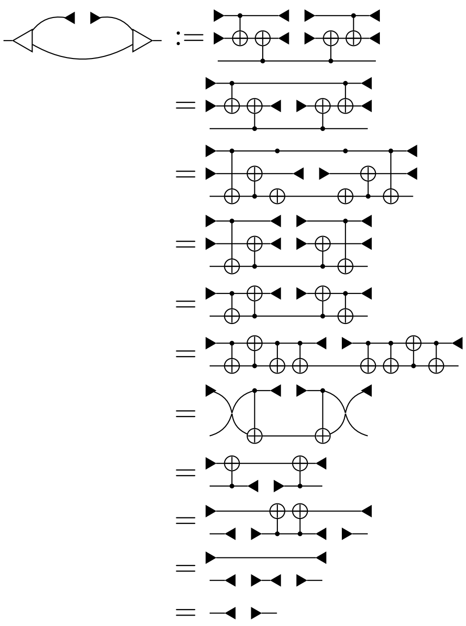
As $\Delta$ is separable

Therefore, latchable circuits are idempotent. □

Before we prove all circuits of the form $ff^\circ$ are latchable, we establish the following identity:

**Lemma B.11.** $\Delta_1(((\langle 1||1\rangle)\otimes 1_1)\nabla_1$

*Proof.* We observe:



□

**Proposition B.12.** *All circuits of the form $ff^\circ$ are latchable.*

*Proof.* We shall prove that all circuits of the form $ff^\circ$ are latchable by induction on the size of $f$.

Any circuit $p$ with $|p| = 0$ is a permutation and, thus, $pp^\circ$ is the identity. So being latchable in this case amounts to separability. Furthermore, adding a permutation, $p$, in front of any latchable circuit, $h$, gives a latchable circuit as:

$$(ph)(ph)^\circ = phh^\circ p^\circ = p\Delta(hh^\circ \otimes 1)\nabla p^\circ = \Delta(phh^\circ p^\circ \otimes pp^\circ)\nabla = \Delta(((ph)(ph)^\circ)\otimes 1)\nabla$$

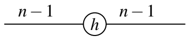
Thus we need only consider adding gates to the top left of circuits: adding a gate anywhere else can be simulated by precomposing with a permutation to move the gates wires to the top, then adding the gate at the top left, and then precomposing with the inverse of the permutation.

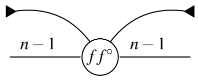
Thus, it suffices to show inductively that when a circuit of the form $ff^\circ$ is latchable, for $|f| < k$, then adding a gate to the top left of $f$ results in a circuit which is still latchable.

**Adding $|1\rangle$:** Given that $n \geq 1$, the symmetric circuit

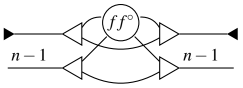
$$h = ((|1\rangle \otimes 1_{n-1})f)((|1\rangle \otimes 1_{n-1})f)^\circ : n-1 \to n-1$$

is latchable, as:

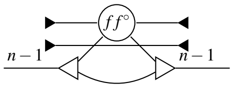


$:=$ 

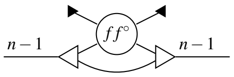
By supposition

$=$ 

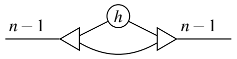
By supposition

$=$ 

Lemma $B$.3

$=$ 

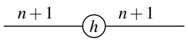
*(CNT.6)*

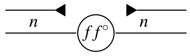
$=:$ 

**Adding $\langle 1|$:** Given that $n \geq 1$, the symmetric circuit

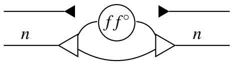
$$h = (((\langle 1| \otimes 1_n)f)(((\langle 1| \otimes 1_n)f)^\circ : n+1 \to n+1$$

is latchable, as:

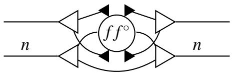


$:=$ 

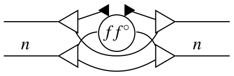
By supposition

$=$ 

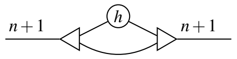
By supposition

$=$ 

As $\Delta$ is natural

$=$ 

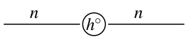
Lemma $B$.11

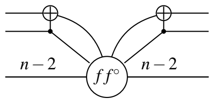
$=:$ 

**Adding cnot:** Given that $n \geq 2$, the symmetric circuit

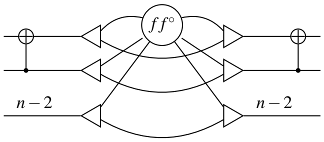
$$h = ((\mathsf{cnot} \otimes 1_{n-2})f)((\mathsf{cnot} \otimes 1_{n-2})f)^\circ : n \to n$$

is latchable, as:

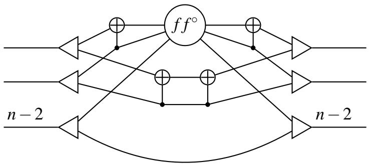


$:=$ 

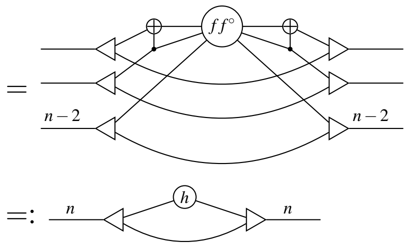
By supposition

$=$ 

By supposition

$=$ 

As $\Delta$ is natural



*(CNT.2)*

Therefore, every circuit of the form $hh^\circ$ is latchable when $|h| = k+1$ completeing the inductive step. □

This allows us to prove that *(Inv.3)* holds:

**Proposition B.13.** *Circuits of the form $ff^\circ$ commute.*

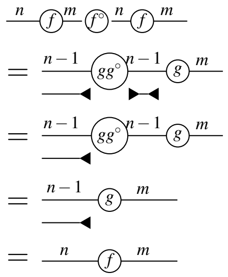
*Proof.* This is immediate from Proposition B.12 and Lemma B.10. □

It remains to prove that *(Inv.2)* holds which we prove by induction.

**Lemma B.14.** *(Inv.2) holds in* CNOT *under the functor* $(\_)^\circ : \mathsf{CNOT}^{op} \to \mathsf{CNOT}$.

*Proof.* We will prove *(Inv.2)* holds under the functor $(\_)^\circ$ by induction on the size of circuits.

- Take $p : n \to n$ to be a circuit with $|p| = 0$. Then $pp^\circ p = p$, since $p$ is a permutation.
- Suppose inductively that *(Inv.2)* holds for all circuits with up to size strictly lesser than $k$. Consider an arbitrary circuit $f : n \to m$ such that $|f| = k$. We proceed by cases:
  - Suppose that $f = (\langle 1| \otimes 1_{n-1})g$. Then:



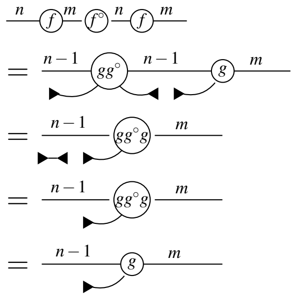
By supposition

*(CNT.6)*

By the inductive hypothesis

By supposition

  - Suppose that $f = (|1\rangle \otimes 1_n)g$. Then:

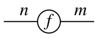


By supposition

*(Inv.3)*

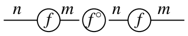
*(CNT.6)*

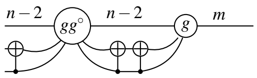
By the inductive hypothesis

= 

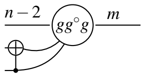
By supposition

- Suppose that $f = (\mathsf{cnot} \otimes 1_{n-2})g$. Then:

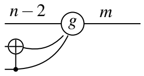


= 

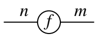
By supposition

= 

*(CNT.2)*

= 

By the inductive hypothesis

= 

By supposition

Therefore, the inductive claim holds.

□

**Theorem B.15.** CNOT *is a discrete inverse category.*

*Proof.* The functor $(\_)^\circ : \mathsf{CNOT}^{\mathrm{op}} \to \mathsf{CNOT}$ which flips circuits horizontally satsifies *(Inv.1)* by construction. It satisfies *(Inv.2)* by Lemma B.14 and *(Inv.3)* is satisfied by Proposition B.13. Hence, CNOT is an inverse category.

CNOT is equipped with a tensor product $\_ \otimes \_ : \mathsf{CNOT} \times \mathsf{CNOT} \to \mathsf{CNOT}$. $\Delta$ is a natural transformation by Lemma B.3, which is cocommutative by Lemma B.4, coassociative by Lemma B.6, a semi-Frobenius algebra by Lemma B.7, and it satisfies *(DInv.4)* by Lemma B.8, where all the dual propositions hold by symmtery. This proves that CNOT has inverse products. Hence, CNOT is a discrete inverse category. □

# C The Equivalence $\mathsf{CNOT} \cong \mathsf{ParIso}(\mathsf{CTor}_2)^*$

The objective of this appendix is to prove that CNOT and $\mathsf{ParIso}(\mathsf{CTor}_2)^*$ are equivalent. The proof involves in five steps:

(1) Defining a functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$, which preserves inverse products.

(2) Showing that $\tilde{H}_0$ is full and faithful on restriction idempotents.

(3) Showing that $\tilde{H}_0$ is essentially surjective.

(4) Showing that $\tilde{H}_0$ is full.

(5) Showing that $\tilde{H}_0$ is faithful.

The key technical steps ((4) and (5) above) are to reduce the full and faithfulness of $\tilde{H}_0$ to its full and faithfulness on restriction idempotents (step (2) above). This latter result is based on the clausal normal form for restriction idempotents in CNOT, which is developed in Section C.2.

## C.1 Defining the functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$

To construct a functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ we consider the following pullback, where $U : \mathsf{CTor}_2 \to \mathsf{Set}$ is the underlying functor:

$$\begin{tikzcd}
\mathsf{ParIso}(\mathsf{CTor}_2)^* \arrow[r, "\mathsf{ParIso}(U)"] \arrow[d, hook] & \mathsf{ParIso}(\mathsf{Set}) \arrow[d, hook] \\
\mathsf{Par}(\mathsf{CTor}_2)^* \arrow[r, "\mathsf{Par}(U)"'] & \mathsf{Par}(\mathsf{Set})
\end{tikzcd}$$

To prove that CNOT is equivalent to $\mathsf{ParIso}(\mathsf{CTor}_2)^*$, the category of partial isomorphisms of finitely generated non-empty commutative torsors of characteristic 2, we start by considering a functor $h_0 : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{Set})$ and on the one hand lift to a functor $H_0 : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{CTor}_2)^*$ and on the other hand lift to a functor $\tilde{h}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{Set})$. Then by the pullback of the diagram $\mathsf{Par}(\mathsf{CTor}_2)^* \xrightarrow{\mathsf{Par}(U)} \mathsf{Par}(\mathsf{Set}) \hookleftarrow \mathsf{ParIso}(\mathsf{Set})$ we are given a unique functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$:

$$\begin{tikzcd}
\mathsf{CNOT} \arrow[drr, bend left, "\tilde{h}_0"] \arrow[ddrr, "h_0"] \arrow[dr, dotted, "\tilde{H}_0"] \arrow[ddr, bend right, "H_0"'] & & \\
& \mathsf{ParIso}(\mathsf{CTor}_2)^* \arrow[r, "\mathsf{ParIso}(U)"] \arrow[d, hook] & \mathsf{ParIso}(\mathsf{Set}) \arrow[d, hook] \\
& \mathsf{Par}(\mathsf{CTor}_2)^* \arrow[r, "\mathsf{Par}(U)"'] & \mathsf{Par}(\mathsf{Set})
\end{tikzcd}$$

The functor $h_0 : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{Set})$ which we shall describe is a restriction hom-functor so we first prove a general result about such functors. Given a restriction category $\mathbb{X}$ and any $X \in \mathbb{X}$, define the following map $h_X := \mathsf{Total}(\mathbb{X})(X, \_) : \mathbb{X} \to \mathsf{Par}(\mathsf{Set})$ as follows:

**On objects:** For each object $Y \in \mathbb{X}$, $h_X(Y) := \{f \in \mathbb{X}(x,y) | \overline{f} = 1_x\}$;

**On maps:** For each map $Y \xrightarrow{f} Z$ in $\mathbb{X}$, for all $g \in h_X(Y)$,

$$(h_X(f))(g) := \begin{cases} gf & \text{if } \overline{gf} = 1_X \\ \uparrow & \text{otherwise} \end{cases}$$

**Lemma C.1.** $h_X : \mathbb{X} \to \mathsf{Par}(\mathsf{Set})$ *is a restriction functor.*

*Proof.* To prove $h_X$ is a restriction functor is to prove $h_X$ preserves identities, composition and restriction structure.

- First, we prove that $h_X$ preserves identities. Take any object $Y \in \mathbb{X}$ and any map $f \in h_X(Y)$. Then, $(h_X(1_Y))(f) = f1_Y = f$ as $\overline{f1_Y} = \overline{f} = 1_X$.
- Next we prove that $h_X$ preserves composition. Consider arbitrary maps $Y \xrightarrow{f} Z \xrightarrow{g} W$ and an $h \in h_X(Y)$.

  Suppose that $\overline{hfg} = 1_X$, then $(h_X(fg))(h) = hfg$ and $\overline{hf} = 1_X$, then

  $$h_X(g)((h_X(f))(h)) = (h_X(g))(hf) = hfg.$$

On the otherhand, suppose that $\overline{hfg} \neq 1_X$ then

$$h_X(g)((h_X(f))(h)) = h_X(g)(\uparrow) = \uparrow$$

If $\overline{hf} = 1_X$, then

$$h_X(g)(h_X(f)(h)) = h_X(g)(hf) = \uparrow .$$

Therefore, $h_X$ preserves composition.

- Finally, we prove that $h_X$ preserves restriction.

  For any $f : Y \to Z$ and any $g \in h_X(Y)$:

$$(h_X(\overline{f}))(g) = \begin{cases} g\overline{f} & \text{if } \overline{g\overline{f}} = \overline{gf} = 1_X \\ \uparrow & \text{otherwise} \end{cases}$$

  However,

$$\overline{h_X(f)}\,(g) = \begin{cases} g & \text{if } (h_X(f))(g)\downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

  But, $(h_X(f))(g)$ if and only if $\overline{gf} = 1_X$ ; moreover if $\overline{gf} = 1_X$, then $g\overline{f} = \overline{gf}\,g = 1_X g = g$. Therefore, $h_X$ preserves restriction.

□

Fixing $\mathbb{X} = \mathsf{CNOT}$ and $X = 0$, we obtain a functor $h_0 := \mathsf{Total}(\mathsf{CNOT})(0,\_) : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{Set})$. As $\mathsf{CNOT}$ is an inverse category, it follows by Lemma C.1 that every map in $h_0(\mathsf{CNOT})$ is a partial isomorphism. Therefore $h_0 : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{Set})$ factors through $\mathsf{ParIso}(\mathsf{Set})$ as $\tilde{h}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{Set})$.

Now that we have the candidate functor $\tilde{h}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{Set})$ for the pullback, we must also show that we can factor $h_0$ through $\mathsf{Par}(U) : \mathsf{Par}(\mathsf{CTor}_2)^* \to \mathsf{Par}(\mathsf{Set})$. To do so, we show that the objects of $\mathsf{CNOT}$ have an internal torsor structure and show that $h_0$ preserves this structure: thus showing it can be factored through $\mathsf{Par}(\mathsf{CTor}_2)^*$. This will allow us to construct the functor $H_0 : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{CTor}_2)^*$ and whence $\tilde{H}_0$.

Proving that $h_0$ is a functor from $\mathsf{CNOT}$ to $\mathsf{Par}(\mathsf{CTor}_2)^*$ is not such a trivial task. To this end, we make several observations regarding maps in the homset $\mathsf{CNOT}(0,n)$ for any $n \in \mathbb{N}$.

To succinctly express total maps $0 \xrightarrow{f} n$ for any $n \in \mathbb{N}$ in $\mathsf{CNOT}$, we define the following family of functions.

**Definition C.2.** *Define a family of functions $|\_\rangle_n : \mathbb{Z}_2^n \to \mathsf{Total}(\mathsf{CNOT})(0,n)$ for all $n \in \mathbb{N}$ as follows.*

*Take $|\rangle := 1_0$. For any $b \in \mathbb{Z}_2^1$ define:*

$$|b\rangle := \begin{cases} |1\rangle & \text{if } n = 1 \\ |0\rangle & \text{otherwise} \end{cases}$$

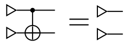
*Moreover, for all $n \in \mathbb{N}$ such that $n > 1$, define:*

$$|b_1, \cdots, b_n\rangle := |b_1\rangle \otimes \cdots \otimes |b_n\rangle$$

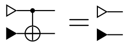
**Lemma C.3.** *Consider a circuit $f : n \to m$ with no output ancillæ. Then, for any $x \in \mathbb{Z}_2^n$, there is some $y \in \mathbb{Z}_2^m$ such that $|x\rangle f = |y\rangle$*

*Proof.* It will suffice to prove our claim for all $b \in \mathbb{Z}_2^n$ on a single controlled-not gate, then by induction, the more general claim follows immediately.

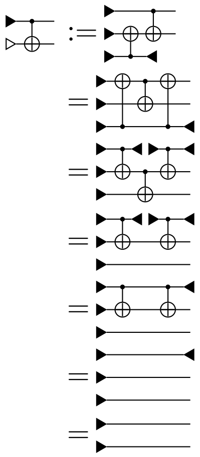
- Take $b = (0,0)$, then by *(CNT.7)*:



- Take $b = (0,1)$, then by *(CNT.7)*:



- Take $b = (1,0)$, then:



*(CNT.8)*

*(CNT.4)*

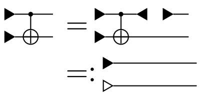
*(CNT.7)*

*(CNT.4)*

*(CNT.2)*

*(CNT.6)*

- Take $b = (1,1)$, then:



*(CNT.4)*

□

The following lemma is an intuitive result which we shall use:

**Lemma C.4.** *For every $f \in \mathsf{CNOT}(0,n)$, $f$ is either total or degenerate (i.e., $\Omega$).*

*Proof.* Consider any circuit $f : 0 \to n$ for any $n \in \mathbb{N}$. We prove that $f$ is either total or degenerate by induction.

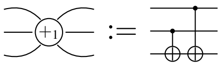
- If $|f| = 0$, then $f$ is a permutation, and is therefore total.
- Inductively suppose that $f$ is either total or degenerate. Consider any circuit $g : n \to m$ such that $|g| = 1$. If $f$ is degenerate, then $fg$ is degenerate as well by Lemma A.4. Otherwise, suppose that $f$ is total. There are three cases:
  - If $|1\rangle \in g$, then $\overline{fg} = \overline{f \otimes g} = \overline{f} \otimes \overline{g} = 1 \otimes 1 = 1$.

- If $\langle 1| \in g$, then the gate to the left of $\langle 1|$ is either $|1\rangle$ or $|0\rangle$. If it is $|1\rangle$, then as $|1\rangle\langle 1| = 1$, it is total. Otherwise, if it is $\langle 1|$, then $|1\rangle\langle 1| =: \Omega$, so $fg$ is degenerate by Lemma A.4.
- If $\mathsf{cnot} \in g$, then $fg$ is total by Lemma C.3.

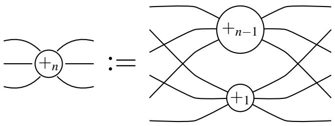
□

To prove that $h_0$ takes maps in $\mathsf{CNOT}$ to well-defined maps in $\mathsf{Par}(\mathsf{CTor}_2)^*$, we construct a torsor-like operation in $\mathsf{CNOT}$ which gives the internal torsor structure which we mentioned above. This will act as the para-multiplication when we project the last 1 out of 3 wires.

**Definition C.5.** *Define a family of maps* $+_n : 3n \to 3n$ *in* $\mathsf{CNOT}$ *inductively such that such that on no wires,* $+_0 := 1_0$. *Furthermore, on one wire:*



*Furthermore, for any* $n > 1$*:*



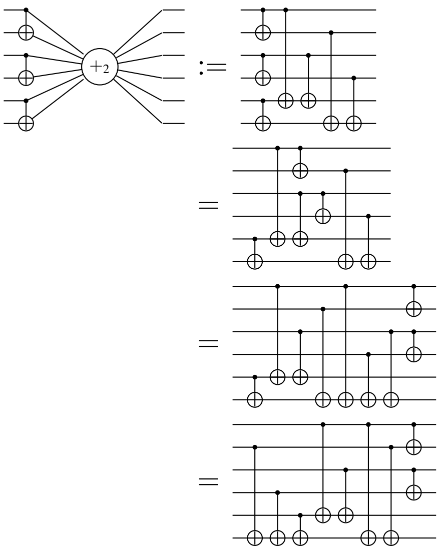
Now we show that $\mathsf{Total}(\mathsf{CNOT})(0,\_)$ really does produces maps which preserve torsor structure.

**Lemma C.6.** *For any map* $f : n \to m$ *in* $\mathsf{CNOT}$, $(f \otimes f \otimes f)+_m = +_n(f \otimes f \otimes f)$.

*Proof.* For any map $f : n \to m$ in $\mathsf{CNOT}$, we prove $\otimes^3 f +_m = +_n \otimes^3 f$ by induction on the size of $f$.

- When $|f| = 0$, $f$ is a permutation, so it is immediate that $\otimes^3 f +_m = +_n \otimes^3 f$.
- Suppose that $\otimes^3 f + = + \otimes^3 f$ for all $|f| \leq k$. Consider some $f : n \to m$ with $|f| = k+1$. We can decompose $f = gh$ for some $|g| = 1$ and $|h| = k$. Note that $\otimes^3 f + = \otimes^3(gh)+ = \otimes^3 g + \otimes^3 h$ by $|f|$. We proceed by cases on the elements of $g$.

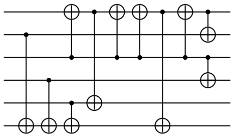
  $\mathsf{cnot} \in g$**:**

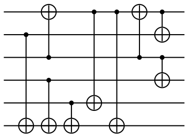


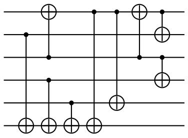
*(CNT.3)*

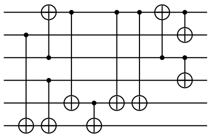
Lemma A.5 (iii) × 2

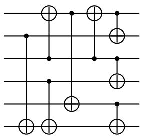
*(CNT.3)* and *(CNT.5)*

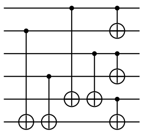
=

*(CNT.8)* $\times 2$

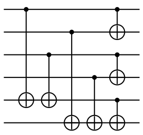
=

*(CNT.2)*

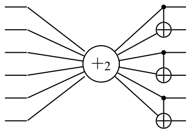
=

*(CNT.3)*

=

*(CNT.8)*

=

*(CNT.2)*

=

*(CNT.8)*

=


=:


Therefore, $\otimes^3 f + = \otimes^3 g + \otimes^3 h = + \otimes^3 (gh) = + \otimes^3 f$

$|1\rangle \in g$ Suppose otherwise that $|1\rangle \in g$. Then by Lemma C.3, $\otimes^3 f + = \otimes^3 g + \otimes^3 h = + \otimes^3 (gh) = + \otimes^3 f$.

$\langle 1| \in g$ If $\langle 1| \in g$, dually to the previous case, $\otimes^3 f + = \otimes^3 g + \otimes^3 h = + \otimes^3 (gh) = + \otimes^3 f$.

□

We also show that $h_0$ produces well defined maps in $\mathsf{Par}(\mathsf{CTor}_2)$.

**Lemma C.7.** *Consider any $n,m \in \mathbb{N}$ and map $f \in \mathsf{CNOT}(n,m)$. For any $x,y,z \in \mathsf{CNOT}(0,n)$ such that $\overline{xf} = \overline{yf} = \overline{zf} = 1_0$, it follows that $\overline{(x \otimes y \otimes z) +_n \otimes^3 f} = 1_0$.*

*Proof.* Consider an arbitrary map $f \in \mathsf{CNOT}(n,m)$ and any $x,y,z \in \mathsf{CNOT}(0,n)$ such that $\overline{xf} = \overline{yf} = \overline{zf} = 1_0$. By Lemma C.6:

$$\begin{aligned}\overline{(x\otimes y\otimes z)+_n\otimes^3 f} &= \overline{(x\otimes y\otimes z)\otimes^3 f+_m} = \overline{(xf\otimes yf\otimes zf)+_m}\\ &= \overline{(xf\otimes yf\otimes zf)\overline{+_m}} = \overline{(xf\otimes yf\otimes zf)1_{3m}}\\ &= \overline{xf\otimes yf\otimes zf} = \overline{xf}\otimes\overline{yf}\otimes\overline{zf} = 1_0\otimes 1_0\otimes 1_0 = 1_0\end{aligned}$$

□

We now prove that $H_0 : \mathsf{CNOT} \to \mathsf{Par}(\mathsf{Tor}_2)^*$ is a functor.

**Lemma C.8.** *$h_0$ can be factored as $H_0\mathsf{Par}(U)$ and $h_0$ preserves torsor structure. Thus,* $\mathsf{CNOT}$ *has internal torsor structure which is preserved by $h_0$.*

*Proof.* First, we prove for every $f : n \to m$ in $\mathsf{CNOT}$, $h_0(f)$ can be regarded as a map in $\mathsf{Par}(\mathsf{CTor}_2)^*$. Consider an arbitrary map $f : n \to m$ in $\mathsf{CNOT}$. If $f$ is degenerate, then $h_0(f)$ vacuously preserves torsor structure. Suppose otherwise that there exists some $x,y,z \in \mathbb{Z}_2^n$ and $x',y',z' \in \mathbb{Z}_2^m$ such that $|x'\rangle = |x\rangle f$, $|y'\rangle = |y\rangle f$ and $|z'\rangle = |z\rangle f$. Forgetting the first 2 out of 3 wires, by Lemma C.7, $h_0(f)(x\oplus y\oplus z)$ is defined; moreover, by Lemma C.6, $h_0(f)(x\oplus y\oplus z) = h_0(f)(x)\oplus h_0(f)(y)\oplus h_0(f)(z)$, so $h_0(f)$ preserves the para-multiplication. □

**Corollary C.9.** *The functor $h_0$ can be lifted to a functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$.*

*Proof.* As $h_0$ can be factored through $\mathsf{ParIso}(\mathsf{Set})$ by Lemma C.1 and $\mathsf{Par}(\mathsf{CTor}_2)^*$ by Lemma C.8, it is also a functor to $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ by pullback. □

**Lemma C.10.** $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ *preserves inverse products.*

*Proof.* We prove that $\tilde{H}_0$ preserves inverse products by the examination of components within $\mathsf{ParIso}(\mathsf{CTor}_2)^*$.

Consider two arbitrary circuits $f : n \to m$ and $f' : n' \to m'$ in $\mathsf{CNOT}$. Moreover, consider any $(b_1,\cdots,b_{n+n'}) \in \mathbb{Z}_2^{n+n'}$. Then by construction of $\tilde{H}_0$:

$$\begin{aligned}\tilde{H}_0(f\otimes g)(b_1,\cdots,b_{n+n'}) &= \tilde{H}_0(|b_1,\cdots,b_{n+n'}\rangle(f\otimes g))(*)\\ &= \tilde{H}_0(|b_1,\cdots,b_n\rangle f)\otimes\tilde{H}_0(|b_{n+1},\cdots,b_{n+n'}\rangle g)(*)\\ &= \tilde{H}_0(|b_1,\cdots,b_n\rangle f\otimes|b_{n+1},\cdots,b_{n+n'}\rangle g)(*)\\ &= (\tilde{H}_0(f)\otimes\tilde{H}_0(g))(b_1,\cdots,b_{n+n'})\end{aligned}$$

Moreover:

$$\tilde{H}_0(f\Delta)(b_1,\cdots,b_{n+n'}) = \tilde{H}_0(f\otimes f)(b_1,\cdots,b_{n+n'}) = (\tilde{H}_0(f)\otimes\tilde{H}_0(f))(b_1,\cdots,b_{n+n'})$$

Therefore, $\tilde{H}_0$ preserves inverse products. □

**Remark C.11.** As mentioned in the main body of the paper, an alternative way to define $\tilde{H}_0$ would be to use the fact that $\mathsf{CNOT}$ is defined freely on gates with relations. Thus, it would have sufficed to provide the interpretation of the gates and then verify the relations. Our proof produces the same functor but it avoids direct verification of the identities. The direct proof may, in fact, be more straightforward; however, some of the lemmas which we have established in our proof will be reused.

As we will reduce the full and faithfulness of $\tilde{H}_0$ to its full and faithfulness on restriction idempotents, the next section is dedicated to describing a normal form for restriction idempotents in $\mathsf{CNOT}$ and establishing the full and faithfulness of $\tilde{H}_0$ on restriction idempotents.

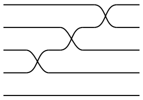
## C.2 Clausal form for restriction idempotents in CNOT

The restriction idempotents of $\mathsf{Par}(\mathsf{CTor})^*$ are determined by finite sets of torsor equations. The restriction idempotents of CNOT also have a normal form, as a conjunction of clauses: we call this the clausal form for restriction idempotents in CNOT. As torsor equations can be translated into clauses it follows that $\tilde{H}_0$ is full on restriction idempotents. Furthermore, by showing that one can perform Gaussian elimination on these clauses we prove that $\tilde{H}_0$ is faithful on restriction idempotents.

**Definition C.12.** *For any $n \in \mathbb{N}$, $1 \le i \le n$, define the map $\mathsf{swap}_{(i,n)} : n \to n$ is a map in* CNOT *inductively as follows:*

$$\mathsf{swap}_{(i,n)} := \begin{cases} 1_n & \textit{If i=0} \\ (1_{n-(i+1)} \otimes \mathsf{swap} \otimes 1_{i-1})(\mathsf{swap}_{(i+1,n)}) & \textit{Otherwise} \end{cases}$$

For example, consider the circuit $\mathsf{swap}_{(4,5)}$:

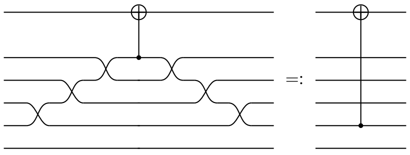


Note that $\mathsf{swap}_{(i,n)}\mathsf{swap}^{\circ}_{(i,n)} : n \to n$ is the identity.

**Definition C.13.** *Given any $n \in \mathbb{N}$ and $1 \le i \le n$, define the **literal** $l_{i,n}$ to be the following:*

$$\mathsf{swap}_{(i,n+1)}\ (\mathsf{cnot} \otimes 1_{n-2})\ \mathsf{swap}^{\circ}_{(i,n+1)}$$

For example, consider the literal $l_{4,5}$:

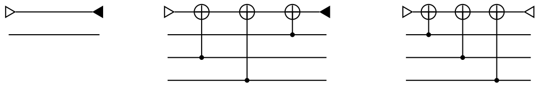


**Definition C.14.** *A **clause** $c : n \to n$ is a map in* CNOT *which is the composition of literals in the following form:*

$$c = (|0\rangle \otimes 1_n) l_{i_1,n} l_{i_2,n} \cdots l_{i_m,n} (a \otimes 1_n)$$

*where $a : 1 \to 0$ is either $\langle 1|$ or $\langle 0|$.*

In a clause, the wire which begins with an input ancillary bit and ends with an output ancillary bit and on which literals act is called the **clause wire**. The following are examples of clauses in which the top wire is the clause wire:

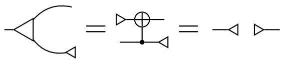


**Definition C.15.** *A map in* CNOT *is said to be in **clausal form** if it can be decomposed into a sequence of clauses.*

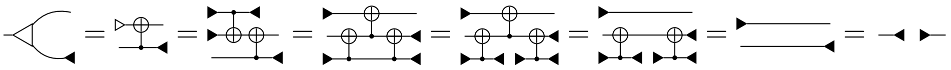
We wish now to show that every restriction idempotent in CNOT can be expressed in clausal form. To achieve this, the following observations are useful:

**Lemma C.16.**

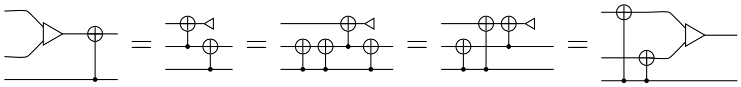
*(i)*



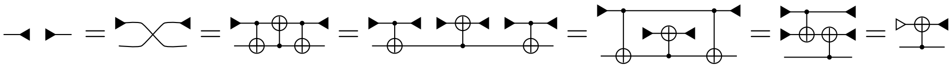
*(ii)*



*(iii)*



*(iv)*



**Lemma C.17.** *In* CNOT *clauses are idempotent.*

*Proof.* To show idempotence of a clause, we describe how to duplicate it. First, using the naturality of $\Delta$, split the input ancilla bit on the clause wire $|0\rangle = (|0\rangle \otimes |0\rangle)\nabla$. Then by repeatedly using Lemma C.16 *(iii)*, copy all of the literals onto both of the new clause wires. Then use the naturality of $\nabla$ on the output ancillary bit $\nabla\langle b| := \langle b| \otimes \langle b|$ to split both clauses apart.

□

**Proposition C.18.** *In* CNOT

*(i) Every restriction idempotent is equivalent to a circuit in clausal form.*

*(ii) Every circuit in clausal form is a restriction idempotent.*

*Proof.*

(i) Given a restriction idempotent $e : n \to n$ for some $n \in \mathbb{N}$, we prove $e$ is in clausal form by induction on the size of the circuit.

- $1_n$ is in clausal form as $1_n = 1_n \otimes 1_0 = 1_n \otimes |1\rangle\langle 1|$.
- Suppose inductively for all circuits $f$ such that $|f| < k$, the restriction idempotent $\overline{f} = ff^\circ$ is in clausal form. Consider some restriction idempotent $f : n \to n$ such that $|f| = k$. Decompose $f$ into circuits $g$ and $h$ such that $|g| = 1$, $|h| = k-1$ and $f = gh$. Consider the three following cases.
  - Suppose that $\langle 1| \in g$.
    Note that $\overline{f} = ff^\circ = ghh^\circ g^\circ = g\overline{h}g^\circ$. The two circuits $g$ and $g^\circ$ form a clause, by Lemma C.16 *(iv)*. Recall that $\overline{h}$ is in clausal form by supposition, as $|h| = k-1 < k$; therefore, $\overline{f}$ is the composition of clauses, and thus a clause itself.

- Suppose that $|1\rangle \in g$.
  As $\overline{f} = ff^\circ = ghh^\circ g^\circ = g\overline{h}g^\circ$ and $\overline{h}$ is in clausal form by Lemma C.3, we push $g$ and $g^\circ$ toward the middle through $\overline{h}$ until the two ancillæ meet and annihilate each other by *(CNT.2)*. This process may have turned some literals into not gates, so slide the not gates to the right side of the clause wires with *(CNT.5)*. This may toggle the output ancillæ on some clause wires; however, as the output ancilla of a clause can be either $\langle 0|$ or $\langle 1|$, $\overline{f}$ is in clausal form.
- Suppose that cnot $\in g$.
  Again, we push both cnot gates inward through $\overline{h}$. If the cnot gates reach each other by *(CNT.2)*, we are done. If this does not happen immediately, as $\overline{h}$ is in clausal form, there are two cases: the control or operating bits may be adjacent to a control bit of a clause. In the first case, the two control bits commute by *(CNT.3)*. In the other case, by Lemma A.5 (iii), we may add another literal to the clause and pass the operating bit through.

(ii) Given a circuit $t = d_1 d_2 \cdots d_m$ in clausal form where $d_1, \cdots, d_m$ are clauses,

$$tt = d_1 \cdots d_m d_1 \cdots d_m = d_1^2 d_2^2 \cdots d_m^2 = d_1 d_2 \cdots d_m$$

as clauses commute by *(CNT.5)* and are idempotent by Lemma C.17. Therefore, as CNOT is an inverse category $t$ is a restriction idempotent.

□

**Theorem C.19.** $\tilde{H}_0$ : CNOT $\to$ ParIso(CTor$_2$)$^*$ *is full and faithful on restriction idempotents.*

*Proof.* A restriction in Par(Tor$_2$) is given by a span in which both legs are equal and, thus, monic. Thus, restrictions correspond precisely to subobjects in Tor$_2$. However, these are determined by sets of torsor equations of the form:

$$\left\{\sum_j b_{i,j} = a_i\right\}_i$$

Each equation, $\sum_j b_{i,j} = a_i$, corresponds in turn to a clause which picks out the wires $b_{i,j}$ and has output ancillary bit $\langle a_i|$. This immediately means that $\tilde{H}_0$ is full on restriction idempotents.

Consider now an arbitrary restriction idempotent expressed as a circuit in clausal form, under $\tilde{H}_0$ it corresponds to a set of equations. We must show that two restriction idempotents in CNOT, whose corresponding sets of equations are equivalent in CTor$_2$, must be equal in CNOT. This amounts to showing that we can perform Gaussian elimination on clauses in CNOT, as two sets of equations are equivalent in CTor$_2$ if and only if they can be shown so by Gaussian elimination steps.

Given two clauses $c$ and $c'$ we show that we can perform the Gaussian elimination step

$$\{c, c'\} \mapsto \{c, c + c'\}$$

and maintain equality.

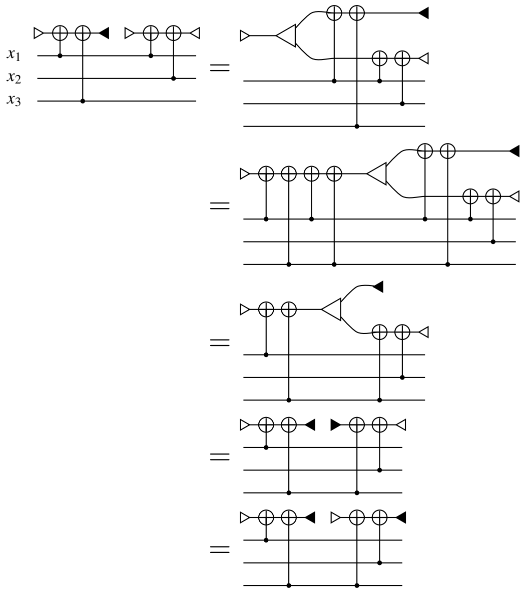
We first join the input ancillæ of both clause wires into $(|0\rangle \otimes |0\rangle) := |0\rangle\Delta$ using naturality of $\Delta$.

By *(CNT.2)*, we copy two copies of each literal in $c$ to the right of the input ancilla. By Lemma C.16 *(iii)* push one copy of each new literal through $\Delta$. On one wire all of the literals will annihilate, and on the other only the common literals between $c$ and $c'$ will annihilate. Use Lemma C.16 (i) and C.16 *(ii)* to split the literals to the left and right of $\Delta$. This may have shifted the input ancilla of the second clause to be $|1\rangle$. In this case, use *(CNT.2)* to push a not gate from the left to right of the clause wire and negate the output ancillary bit of the second clause. The result is two clauses corresponding to the Gaussian elimination step. Therefore, we can perform Gaussian elimination on clauses in $\mathsf{CNOT}$.

For example, suppose we are given a circuit determined by the equations:

$$\begin{bmatrix}1 & 0 & 1\\ 1 & 1 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}=\begin{bmatrix}1\\ 0\end{bmatrix}$$

We can perform Gaussian elimination as follows



(CNT.2)

Lemma C.16, (CNT.2)

Lemma $C.16(ii)$

Which represents the reduced system of linear equations:

$$\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 1\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix}=\begin{bmatrix}1\\ 1\end{bmatrix}$$

Hence, if the image of two circuits are equal under the functor $\tilde{H}_0$, then they are the same. □

## C.3 $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ is essentially surjective

In order to prove that $\tilde{H}_0$ is essentially surjective, we invoke the alternative characterization of $\mathsf{CTor}_2$ given by Proposition 3.3.

**Proposition C.20.** *$\tilde{H}_0$ is essentially surjective.*

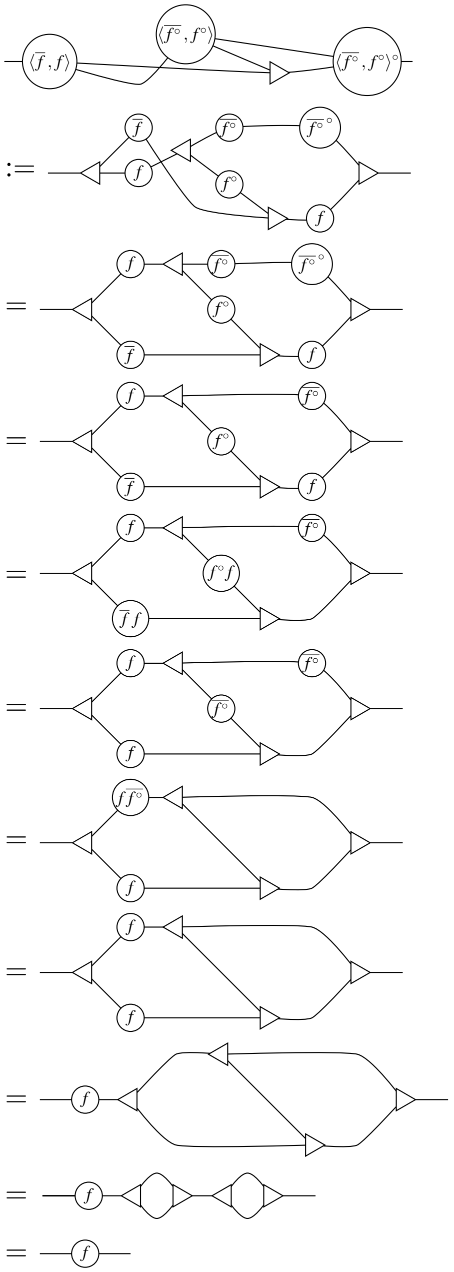
*Proof.* Consider any torsor $(X,\times)$ in $\mathsf{ParIso}(\mathsf{CTor}_2)^*$. There is some $n \in \mathbb{N}$ such that $(X,\times) \cong (\mathbb{Z}_2^n, \_\oplus\_\oplus\_)$ by Proposition 3.3. However, $\mathsf{Total}(\mathsf{CNOT})(0,n) = \mathbb{Z}_2^n$. □

## C.4 $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ is full

In order to prove that $\tilde{H}_0$ is full, we will prove two useful results:

**Lemma C.21.** *Let $F : \mathbb{X} \to \mathbb{Y}$ be an inverse product preserving functor between discrete inverse categories. Let $f$ be a partial isomorphism in $\mathbb{Y}$. If $\langle \overline{f}, f \rangle := \Delta(\overline{f} \otimes f)$ and $\langle \overline{f^\circ}, f^\circ \rangle := \Delta(\overline{f^\circ} \otimes f^\circ)$ are in the image of $F$, then $f$ and $f^\circ$ are also in the image of $F$.*

*Proof.* Observe that in $\mathbb{Y}$ we have:



$\langle \overline{f}, f \rangle$
$\langle \overline{f^\circ}, f^\circ \rangle$
$\langle \overline{f^\circ}, f^\circ \rangle^\circ$
:=
$f$
$\overline{f}$
$\overline{f^\circ}$
$\overline{f^\circ}^\circ$
$f^\circ$
$f^\circ f$
$\overline{f} f$
$f \overline{f^\circ}$
=

As $\Delta$ is cocommutative

As $\Delta$ is natural

As $\Delta$ is natural

As $\Delta$ is natural

By the semi-Frobenius property

As $\Delta$ is separable

Therefore, $f \in F(\mathbb{X})$ and by symmetry $f^\circ \in F(\mathbb{X})$ as well.

□

**Lemma C.22.** *If $f \in \mathsf{CTor}_2(\mathbb{Z}_2^n, \mathbb{Z}_2^m)$, then there is a map $g \in \mathsf{CNOT}(n,m)$ with $\tilde{H}_0(g) = \langle 1, f \rangle$.*

*Proof.* Consider $f \in \mathsf{CTor}_2(\mathbb{Z}_2^n, \mathbb{Z}_2^m)$. Recall that $f$ may be regarded as a linear map $t : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ with a shift $(b_1, \cdots, b_m)$. Consider the standard bases $\{e_i\}$ and $\{m_j\}$ of $\mathbb{Z}_2^n$ and $\mathbb{Z}_2^m$, respectively. As $t$ is a linear map, for any $1 \leq i \leq n$ there are unique coefficients $a_{i,j} \in \mathbb{Z}_2$ for all $1 \leq j \leq n$ such that:

$$f(e_i) = \sum_{i=1}^{m} a_{i,j} m_i$$

However, as $\mathbb{Z}_2^n$ is a vector space over $\mathbb{Z}_2$, the coefficients $a_{i,j}$ are either 0 or 1 so they determine for each $i$ a subset of the $m_i$.

Construct a circuit by starting with $1_n \otimes |b_1, \cdots, b_m\rangle$ and condition on $a_{ij}$; apply a $\mathsf{cnot}$ gate from the $i$th wire to the $i+j$th wire for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Call this new circuit $g$. Given any $(c_1, \cdots, c_n) \in \mathbb{Z}_2^n$, by Lemma $C$.3:

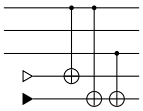
$$|c_1, \cdots, c_n\rangle g = \bigotimes_{j=1}^{m} \left| b_j + \sum_{i=1}^{n} a_{i,j} c_i \right\rangle$$

Therefore, $\tilde{H}_0(g)(c_1, \cdots, c_n) = f(c_1, \cdots, c_n)$ and thus $\tilde{H}_0(g) = f$.

For example, consider the map $f \in \mathsf{CTor}_2(\mathbb{Z}_2^3, \mathbb{Z}_2^2)$ given by the affine transformation with a linear component $T$ and shift $S$ such that:

$$T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \qquad \text{and} \qquad S = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Then the corresponding circuit $g$ such that $\tilde{H}_0(g) = \langle 1, f \rangle$ is:



□

We are now ready to prove:

**Proposition C.23.** $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ *is full.*

*Proof.* Suppose $A \xleftarrow{f} A' \xrightarrow{g} B$ is a partial isomorphism in $\mathsf{Par}(\mathsf{CTor}_2)^*$. Thus $f$ and $g$ are monics. If $A'$ is empty we can simulate the map as $\tilde{H}_0(\Omega_{n,m})$ for some $n, m \in \mathbb{N}$. On the otherhand if $A'$ is non-empty then there is a total map $r$ with $fr = 1_{A'}$ as the object $A'$ is injective (as it is injective as a $\mathbb{Z}_2$-vector space). This means the total map $A =\!=\!= A \xrightarrow{rg} B$ extends $(f, g)$ (so $(f, g) \leq (1_A, rg)$) as

$$\begin{tikzcd}
& A' \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[dd, "f"] & \\
A \arrow[dr, equal] & & B \\
& A \arrow[ur, "rg"'] &
\end{tikzcd}$$

But by Lemma C.22 there is a map $k \in \mathsf{CNOT}$ with $\tilde{H}_0(k) = \langle 1, rg \rangle$. By the fullness of $\tilde{H}_0$ on restriction idempotents there is an $e$ with $\tilde{H}_0(e) = (f, f)$ but then

$$\tilde{H}_0(ek) = \tilde{H}_0(e)\tilde{H}_0(k) = (f,f)\langle 1_a, rg\rangle = \langle \overline{(f,g)}, (f,g)\rangle.$$

Similarly we can implement $\langle \overline{(g,f)}, (g,f)\rangle$ and therefore by Lemma C.21 we can implement $(f,g)$.

Thus $\tilde{H}_0$ is full. □

## C.5 $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ is faithful

We reduce the faithfulness of $\tilde{H}_0$ to being faithful on restriction idempotents in two stages.

**Lemma C.24.** *A restriction functor $F : \mathbb{X} \to \mathbb{Y}$ between inverse categories is faithful if and only if it reflects and is faithful on restriction idempotents.*

To reflect restriction idempotents means that, whenever $h : A \to A$ is an endomorphism with $F(h)$ a restriction idempotent, then $h$ is a restriction idempotent itself.

*Proof.*

$\Rightarrow$ : Suppose $F$ is faithful then it is faithful on restriction idempotents. If $F(g) = \overline{F(g)}$, then $F(g)F(g) = F(gg) = F(g)$. So $g$ is an idempotent and thus a restriction idempotent (as all idempotents are restriction idempotents in an inverse category).

$\Leftarrow$ : Suppose $F$ reflects and is faithful on restriction idempotents and that $F(f) = F(g)$ for $f, g$ which are parallel maps in $\mathbb{X}$. This means that

$$\overline{F(f)} = F(f)F(f)^\circ = F(f)F(g)^\circ = F(fg^\circ)$$

So $fg^\circ$ is a restriction idempotent as is $g^\circ f$. But

$$F(fg^\circ) = F(f)F(g)^\circ = F(f)F(f)^\circ = F(ff^\circ)$$

So $fg^\circ = ff^\circ$. Thus $g^\circ$ is the partial inverse of $f$, and hence $g^\circ = f^\circ$.

□

Therefore, as $\tilde{H}_0$ is a restriction functor, it suffices to prove that $\tilde{H}_0$ reflects and is faithful on restriction idempotents. However, we can do better for discrete inverse categories:

**Lemma C.25.** *A restriction functor $F : \mathbb{X} \to \mathbb{Y}$ between discrete inverse categories which preserves the inverse product is faithful if and only if it is faithful on restriction idempotents.*

*Proof.*

$\Rightarrow$ : If $F$ is faithful it is certainly faithful on restriction idempotents.

$\Leftarrow$ : By Lemma C.24, it suffices to prove that $F$ reflects restriction idempotents.

Suppose $F(f) = F(\overline{f})$, then

$$F(\overline{f}) = F(f) \cap \overline{F(f)} = F(f) \cap F(\overline{f}) = F(f \cap \overline{f})$$

Since $\overline{f}$ and $f \cap \overline{f}$ are restriction idempotents and $F$ is faithful on restriction idempotents, then $\overline{f} = f \cap \overline{f} \leq f$. But then $\overline{f} \leq f$ iff $\overline{f}f = \overline{f}$. So $f = \overline{f}$ as $\overline{f}f = f$.

□

Therefore, by Lemma C.25 and Lemma C.10, it suffices to show that $\tilde{H}_0$ is faithful on restriction idempotents to prove that it is faithful. However, we already have proven that $\tilde{H}_0$ is faithful on idempotents in Theorem C.19 so we have:

**Proposition C.26.** $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ *is faithful.*

Finally this gives the main theorem:

**Theorem C.27.** *There is an equivalence of categories between* $\mathsf{CNOT}$ *and* $\mathsf{ParIso}(\mathsf{CTor})^*$.

*Proof.* The equivalence functor $\tilde{H}_0 : \mathsf{CNOT} \to \mathsf{ParIso}(\mathsf{CTor}_2)^*$ is full, faithful, and essentially surjective by Propositions C.23, C.26 and C.20, respectively. □